Service Description

IBM Managed Security Services for Unified Threat Management

1. Service Overview

IBM Managed Security Services for Unified Threat Management (called "MSS for UTM") is designed to provide a comprehensive security solution deployed across a variety of Appliances.

MSS for UTM is intended to be a comprehensive security service, divided into two distinct packages:

- Protection Package - includes Intrusion Prevention system ("IPS") and firewall support, and helps block traditional attacks such as worms and intruders; and
- Content Package - includes management of, and support for, Web filtering, antispam, and antivirus modules. This package helps Customers eliminate unsolicited e-mails and objectionable Web content, while providing protection from newer threats such as identity theft ("phishing"), viruses, and spyware.

IBM offers each MSS for UTM package at the following alternative service levels.

- MSS for UTM – Standard;
- MSS for UTM – Select; and
- MSS for UTM – Premium,

each described in further detail below.

The details of your order (e.g., the services you require (including service levels), contract period, and charges) will be specified in the Order.

Definitions of service-specific terminology can be found at www.ibm.com/services/iss/wwcontracts

IBM will support the following product features, as applicable:

a. Intrusion Detection and Intrusion Prevention system ("IDS/IPS")

IDS/IPS is a security management system for computers and networks that is designed to gather and analyze information from various areas within a computer or a network, to help identify and block possible security breaches (i.e., intrusions (attacks from outside the organization) and misuse (attacks from within the organization)).

b. firewall

A firewall is a set of related programs, located at a network gateway server that is designed to allow or deny certain Hosts or networks to speak to each other, based on a set security policy. Many firewalls include a full set of networking features (e.g., routing capabilities and address and port rewriting).

c. VPNs

VPNs allow supported firewall-based VPNs to be connected to the managed Agent. IBM will configure the managed Agent to support site-to-site or client VPN tunnels.

d. high availability

To help protect against hardware failure and provide high availability, two managed protection Agents may be configured and deployed; one fully operational and the other waiting as a backup to take over should the first Agent fail. Some Agents can also be deployed as clusters, such that both Agents operate and share network load.

e. antispam

Antispam technology is designed to minimize the volume of spam e-mail to user mail boxes. Spam filters utilize spam signatures, detection algorithms, and heuristic analysis to reduce the volume of unwanted e-mail and help remove objectionable content.

f. Web filtering

Web filtering helps the Customer to block objectionable content, mitigate Web-borne threats, and govern Web viewing behavior of personnel behind the managed Agent.

g. antivirus

Gateway antivirus systems scan many kinds of file transfers such as Web pages, e-mail traffic, and file transfer protocol ("FTP") exchanges for worms, viruses, and other forms of malware.

IBM will provide the following services in support of the product features listed above, as applicable:

h. project kickoff, assessment, and implementation

During deployment and initiation of MSS for UTM, IBM will work with the Customer to help define appropriate security policies, assist with installation and configuration of the Agent(s), and verify proper device operation prior to transition of the firewall(s) to the SOC.

i. policy management

Firewalls only protect Hosts when configured correctly for their network environment. IBM provides policy management services to help the Customer keep firewalls configured with a valid security policy, and IBM retains records of all changes.

j. device management

IBM will maintain the firewall by monitoring its system health and availability and applying vendor updates to the firewall.

k. security event monitoring

Unified threat management devices (called "UTMs") are capable of generating a high volume of alerts in response to the security conditions for which they are configured. The actual security risk corresponding to a particular condition detected by a firewall is not always clear, and it is not practical to block all data that may be harmful, as the default. Additional monitoring and analysis provided by IBM security analysts on a 24 hours/day by 7 days/week basis helps cover this security gap by maintaining a focus on alerts which may be significant, validating these alerts as probable Security Incidents and escalating the probable Security Incidents to the Customer.

l. vulnerability management

Vulnerabilities are weaknesses in Hosts in the Customer's environment, and IBM will provide vulnerability management services to help identify and remediate these vulnerabilities.

m. X-Force Threat Analysis Service

IBM will provide security intelligence to the Customer based on such things as original research completed by the IBM X-Force® research and development team, worldwide threat activity as identified by the IBM Global Threat Operations Center, and secondary research from other public and private resources.

n. Virtual-SOC

The Virtual-SOC is a Web interface which serves as the Customer's interface to management of the firewall, alerts, logs, reports, policy change requests, and other types of service tickets.

The following table provides an overview of the MSS for UTM product features for the Protection and Content packages.

Table 1 - MSS for UTM Packages

Product Features	Included as part of Protection package? (Yes or No)	Included as part of Content package? (Yes or No)	Included if Customer subscribes to both packages? (Yes or No)
Intrusion Prevention management	Yes	No	Yes
Firewall and VPN management	Yes	No	Yes
Web filter management	No	Yes	Yes
Antispam management	No	Yes	Yes
Antivirus management	No	Yes	Yes

The following table provides an overview of the MSS for UTM product features for the Standard, Select, and Premium service levels.

Table 2 - Product Features

Feature	Standard Level	Select Level	Premium Level
VPN Support • site-to-site • client/SSL	 • Up to 2 tunnels • Up to 20 users online at any time	 • Up to 2 tunnels • Up to 50 users online at any time	 • Unlimited • Unlimited

The following table provides an overview of the MSS for UTM services, for the Standard, Select, and Premium service levels, provided in support of the product features listed above.

Table 3 - Services

Service	Standard Level	Select Level	Premium Level
Project kickoff, assessment, and implementation	Included	Included	Included
Supported bandwidth (firewall-only throughput)	Up to 100 Mbps	500 Mbps	1 Gbps and up
Policy management • Policy and configuration changes for 1 package • Policy/configuration maintenance window • Extra policy changes with 2nd package • Number of policies	 • 2 per month • No • 1 • 1 per port	 • 4 per month • Yes • 1 • 1 per port	 • Unlimited • Yes • N/A • 1 per port pair
Device Management • Log Storage/Availability • Application/Operating System Upgrades • Out of Band	 • Up to 1 year • Yes • Optional	 • Up to 7 years • Yes • Required	 • Up to 7 years • Yes • Required
Security event monitoring	Automated monitoring	Automated monitoring plus optional real-time 24x7 human analysis	Automated monitoring plus optional real-time 24x7 human analysis
Vulnerability management	Quarterly scan of 1 IP	Quarterly scan of 2 IPs	Quarterly scan of 3 IPs
IBM Internet Security Systems™ X-Force® Threat Analysis Service	1 seat for the X-Force Threat Analysis Service security intelligence service		
Virtual-SOC	Provides real-time access for communications		

MSS for UTM – General Terms

MSS for UTM is comprised of two different packages (Protection and Content) with each package offered at three different service levels (Standard, Select, and Premium). Customers requiring both packages must contract for them at the same service level.

2. IBM Responsibilities

2.1 Deployment and Initiation

The terms and conditions set forth in this section entitled “Deployment and Initiation” apply to both packages (Protection and Content) at all three service levels (Standard, Select, and Premium).

2.1.1 Data Gathering

During deployment and initiation, IBM will work with the Customer to deploy a new Agent or begin management of an existing Agent.

2.1.2 Project Kickoff

IBM will send the Customer a welcome e-mail and conduct a kickoff call to:

- introduce the Customer contacts to the assigned IBM deployment specialist;
- set expectations; and
- begin to assess the Customer requirements and environment.

IBM will provide a document called "Network Access Requirements", detailing how IBM will connect remotely to the Customer's network, and any specific technical requirements to enable such access. Typically, IBM will connect via standard access methods through the Internet; however, a site-to-site VPN may be used, if appropriate.

2.1.3 Assessment

Data Gathering

IBM will provide a form for the Customer to document detailed information for the initial setup of the Agent and associated service features. Most of the questions will be technical in nature and help determine the layout of the Customer network, Hosts on the network, and desired security policies. A portion of the requested data will reflect the Customer organization, and will include security contacts and escalation paths.

Environment Assessment

Using the provided information, IBM will work with the Customer to understand the existing Customer environment, and build a configuration and security policy for the Agent. If migrating from an existing Agent to a newer Agent, IBM will use the configuration and policy on the existing Agent.

During this assessment, IBM may make recommendations to adjust the policy of the Agent or the layout of the network to enhance security. IBM recommends that all Agents be deployed inline, at the network perimeter. If an Agent does not include firewall capabilities, or is implemented with firewall capabilities disabled, IBM recommends that the Agent be deployed behind a firewall. Placement outside the firewall may require policy tuning to eliminate high volumes of false alarms and may limit IBM's ability to implement certain protection strategies.

If the Customer chooses to deploy the Agent in a passive mode, the protection provided by the Agent will be substantially decreased. Should the Customer choose to transition to an inline deployment at a later date, this transition will require advance notice due to the extra effort that will be required.

IBM will work with the Customer to help determine an optimal Agent configuration based on the Customer's network and firewall configuration, and the most active worldwide threats (as determined by the IBM Global Threat Operations Center). IBM may tune the policy to reduce the number of erroneous alarms, if required.

Existing Agent Assessment

If IBM will be taking over management of an existing Agent, IBM must assess the Agent to be sure it meets certain specifications. IBM may require the Agent software or Security Content to be upgraded to the most current versions in order to provide the service. Other required criteria may include the addition or removal of applications and user accounts.

2.1.4 Implementation

Configuration at IBM

For Agents purchased through IBM at the time of deployment, much of the configuration and policy setting will take place at IBM facilities. For existing Agents already in use, the Customer will have the option to ship the Agent to IBM for configuration at IBM facilities.

Installation

While physical installation and cabling are a Customer responsibility, IBM will provide live support, via phone and e-mail, and will assist the Customer with location of vendor documents detailing the installation procedure for the Agent. Such support must be scheduled in advance to ensure availability of a deployment specialist.

At the Customer's request, physical installation may be provided by IBM Professional Security Services ("PSS") for an additional fee.

Remote Configuration

When taking over management of an existing Agent, IBM will typically perform the configuration remotely. The Customer may be required to physically load media.

All managed Agents will require some remote configuration, which may include the registration of the Agent with IBM Managed Security Services infrastructure.

2.1.5 Transition to SOC

Once the Agent is configured, physically installed and implemented, and connected to the IBM Managed Security Services infrastructure, IBM will provide the Customer with the option of having a demonstration of the Virtual-SOC capabilities and performance of common tasks.

The final step of services deployment is when the SOC takes over management and support of the Agent and the relationship with the Customer. At this time, the ongoing management and support phase of the services officially begins. Typically, IBM will introduce the Customer via phone to the SOC personnel.

2.2 Ongoing Management and Support - General

Except as specifically stated below, the terms and conditions set forth in this section entitled "Ongoing Management and Support - General" apply to both packages (Protection and Content) at all three service levels (Standard, Select, and Premium).

IBM will provide MSS for UTM services during the initial contract term after the services environment has been established, and during any renewal contract term.

2.2.1 Policy Management

Based on the security policy and configuration developed during deployment and initiation, IBM will maintain a sound security policy for all Agent features under IBM management.

Changes

All policy and configuration changes for managed Agent features will be completed only by IBM.

Customers who subscribe to one package (either Protection or Content) may request policy changes (as specified below) by submitting a policy change request through the Virtual-SOC. The allowed number of policy changes is as follows:

- Standard level – up to two policy changes per calendar month
- Select level - up to four policy changes per calendar month
- Premium level – unlimited policy changes per calendar month

Customers who subscribe to both the Protection and Content packages, at either the Standard or Select level, may request one additional change per month beyond the allowed number indicated above.

Additional policy changes can be provided for an additional fee. Following the closure of a calendar month, unused policy changes are considered void and may not be rolled over to the following month.

Maintenance Windows

Additionally, Customers at the Select or Premium service level may specify a time period for IBM to implement a single policy or configuration change. The Customer may specify a start time, and optionally, an end time for the window, but the window must be at least 30 minutes long.

If the Customer does not specify an end time for this maintenance window, IBM will begin implementation of the requested policy change within 30 minutes of the window start time. If the Customer specifies a start and end time, IBM will begin implementation of the policy change within the maintenance window.

Emergency Policy Changes

Customers at the Premium service level may request one emergency change per month, for each IBM-managed Agent, for the duration of the contract. Unused emergency changes do not roll over to the following calendar month.

Customers at the Standard and Select service levels will be provided with emergency policy changes for an additional fee.

To submit an emergency change request, Customers must submit the change request through the Virtual-SOC, following normal change submission procedures. During the electronic submission of the

change request, the change must be clearly identified as an emergency. Following electronic submission, an authorized security contact must place a follow-up phone call to the SOC and escalate the change submission to emergency status.

Reporting

The Customer will have access to comprehensive service information, via the Virtual-SOC, to review service tickets and Security Incidents at any time. Once per month, IBM will produce a summary report that includes:

a. number of SLAs invoked and met;

b. number and type of service requests;

c. list and summary of service tickets;

d. number of Security Incidents detected, priority and status; and

e. list and summary of Security Incidents.

2.2.2 Device Management

IBM will be the sole provider of software-level device management for the Agent. With root/super-user/administrator level access to the device, along with an out-of-band system and an Agent installed on the device, IBM will maintain system status awareness, apply operating system patches and upgrades, troubleshoot problems on the device, and work with the Customer to help ensure the device remains available. IBM will monitor for availability of the Agent, notify the Customer when certain utilization thresholds have been met, and monitor the device 24 hours/day by 7 days/week.

Regular, automatic updates will be provided for the software and firmware.

On-site assistance can be provided by IBM PSS for an additional fee.

Management Connectivity

All security logs, events and management data travel between the SOC and the managed Agent via the Internet. Data traveling across the Internet is encrypted using industry-standard strong encryption algorithms whenever possible.

Requests for connectivity through alternate means (e.g., private data circuit and/or VPN) will be addressed on a case-by-case basis. Additional monthly fees may apply to accommodate connection requirements outside of the standard in-band connectivity.

Management Platforms

In many cases, IBM will use a management platform on IBM premises to manage the Agent.

For IBM Proventia® products, IBM will typically use the IBM SiteProtector™ management infrastructure to control Agent policy and configuration, to push updates to the Agent, and to securely receive data from the Agent using a SiteProtector event collector (called “Event Collector”).

In some cases, the Customer may already use SiteProtector, and may choose to connect the Agent to the Event Collector on their premises. The Customer’s Event Collector will then connect to the SiteProtector infrastructure at IBM. This configuration is commonly known as “stacking”. Any Customer choosing to use a stacked SiteProtector configuration will be subject to additional responsibilities.

Log Storage

The X-Force® Protection System (“XPS”) serves as a data warehouse for event data from a variety of security devices, applications, and platforms. Following display on the Virtual-SOC, logs are migrated to a physical backup media such as tape or DVD. Backup media is archived in a secure, environmentally controlled facility. Archived data will be available for a user-defined time period not to exceed seven years from the date of log creation.

At the Customer’s request, IBM will submit a request for media location and retrieval. Hourly consulting fees will apply for all time spent restoring and preparing data in the Customer’s requested format.

Health and Availability Monitoring

The health and performance of MSS for UTM is monitored by using a Host-based monitoring Agent (when possible) or SNMP. The devices are regularly polled by the SOC, keeping IBM security analysts informed of potential problems as they develop. Key metrics analyzed by the monitoring Agent include:

- hard disk capacity (if applicable);

- CPU utilization;
- memory utilization; and
- process availability.

In addition to system health metrics, IBM will monitor device availability. If contact with a managed device is lost, additional time-based checks will be initiated to verify a valid outage has been identified.

In the event system health problems or an outage has been confirmed, a trouble ticket will be created and an IBM security analyst will be notified to begin research and investigation. The status of all system health tickets is available through the Virtual-SOC.

Outage Notification

If the Agent is not reachable through standard in-band means, the Customer will be notified via telephone using a predetermined escalation procedure. Following telephone escalation, IBM will begin investigating problems related to the configuration or functionality of the managed device.

Application/Operating System Updates

Periodically, it will be necessary for IBM to install patches and software updates to improve device performance, enable additional functionality, and resolve potential application problems. The application of such patches and updates may require platform downtime or Customer assistance to complete. If required, IBM will declare a maintenance window in advance of any such updates, and the notification will clearly state the impacts of the scheduled maintenance and any Customer-specific requirements.

Security Content Updates

To help ensure that the most current threats are properly identified, IBM will periodically update security platforms with the most current Security Content. Security Content, delivered in the form of new checks or signatures for the IPS, antispam and antivirus modules, and new URL listings for the Web filtering module, enhances the Agent's security capabilities.

At the discretion of IBM, Security Content updates may be downloaded and installed onto the security platform at any time. Such an operation is transparent to users.

Device Troubleshooting

If the Agent does not perform as expected, or is identified as the potential source of a network-related problem, IBM will examine the device configuration and functionality for potential issues. Troubleshooting may consist of an offline analysis by IBM, or an active troubleshooting session between IBM and the Customer. IBM will attempt to resolve any technical issues as expediently as feasible. If the Agent is eliminated as the source of a given problem, no further troubleshooting will be performed by IBM.

Out-of-Band Access

Out-of-band ("OOB") access is a highly recommended feature that assists the SOC in the diagnosis of potential device issues. Implementing OOB requires the Customer to purchase an IBM-supported OOB device and provide a dedicated analog phone line for connectivity.

OOB is an optional feature at the Standard level of service, but required for the Select and Premium levels.

If the Customer has an existing OOB solution, IBM will use this solution for OOB access to managed devices, provided:

- the solution does not allow IBM access to any non-managed devices;
- using the solution does not require installation of any specialized software;
- the Customer provides detailed instructions for accessing IBM-managed devices; and
- the Customer is responsible for all aspects of managing the OOB solution.

2.2.3 Vulnerability Management

The vulnerability management service is a remotely delivered, electronic service that regularly and automatically scans the Customer's Internet perimeter devices for known vulnerabilities. Each scan results in several comprehensive reports that are designed to identify potential weaknesses, assess relative network risk, and provide recommendations to manage identified vulnerabilities. IBM will require the Customer to validate they are the owner of the IP address range to be scanned, prior to the initial scan of such IP address range being performed. For each Agent purchased, the Customer will receive quarterly remote vulnerability assessment scanning for one IP address.

Features of the vulnerability management service include:

a. External vulnerability management - IBM will provide external vulnerability management for each Agent under full management. This includes one quarterly scan of the Host's Internet accessible IP addresses, for the duration of the contract.

b. Vulnerability discovery - IBM scanners are designed to detect a large set of vulnerabilities on a wide variety of Hosts.

c. Prioritization - IBM catalogs each scanned device (asset) and allows Customers to assign business criticality ratings and system owners to specific assets. This allows IBM to notify asset owners when vulnerabilities are identified, and facilitates establishment of a personalized view into overall program impacts on security posture.

d. Remediation - identified vulnerabilities can be assigned to designated asset owners for review and remediation. The individual asset owners are provided with access to use the Virtual-SOC as a tool for learning about a specific vulnerability, and tracking its remediation within the enterprise.

e. Dynamic protection - vulnerability management capabilities can integrate with a Customer's existing IBM Managed Security Services to dynamically request the update of server and network IPS policies with appropriate blocking responses.

f. Verification – after an asset owner indicates a vulnerable application or system has been effectively patched, the assignment is designed to remain active until the scanning system verifies known attack vectors for a given vulnerability have been successfully eliminated.

g. Customized reporting - IBM provides reports of service performance and security posture, either in a stand-alone presentation, or combined with data from multiple IBM Managed Security Services.

2.2.4 High Availability

High availability ("HA") increases the reliability of MSS for UTM by supporting the implementation of redundant Agents into your managed environment. Adding HA to the service may require changes to the Agent, software licensing, IP addressing requirements, or managed services fees. MSS for UTM does not support non-integrated, third party HA solutions.

Active/Passive Implementations

Active/passive implementations improve reliability of the Agent gateway solution through redundancy. In this configuration, a second Agent is configured as a hot-standby, ready to begin serving the network if the primary Agent experiences a critical hardware or software failure. In such a scenario, failover is designed to be automatic and nearly instantaneous. Active/passive configurations are recommended for mission critical environments with low to medium traffic loads.

Active/Active Implementations

Active/active clusters improve reliability and performance of the managed Agents by using both Agents to handle the network traffic simultaneously. In this configuration, each Agent handles a share of the network packets, determined by a load-balancing algorithm. If one Agent fails, the other Agent is designed to automatically handle all of the traffic until the failed Agent has been restored. Active/active configurations are recommended for mission critical environments with high traffic volumes and/or large fluctuations in network utilization.

2.2.5 X-Force Threat Analysis Service

X-Force Threat Analysis Service provides proactive security management through comprehensive evaluation of global online threat conditions and detailed analyses.

The service provides threat information collected from the SOCs, trusted security intelligence from the IBM X-Force® research and development team and from the IBM Global Threat Operations Center, and secondary research from other public and private resources. This combination helps to identify the nature and severity of external Internet threats. In addition to alerts and X-Force intelligence, each registered security contact will receive detailed information regarding real-time Internet port metrics, Web defacements, worms and virus activity, as well as daily analysis of Internet threat conditions.

For each Agent purchased, the Customer will receive one seat for the X-Force Threat Analysis Service for the duration of the contract.

2.2.6 Virtual-SOC

The Virtual-SOC is a Web-based interface designed to enable delivery of key service details and on-demand protection solutions. The Virtual-SOC is structured to deliver a consolidated view of the Customer's overall security posture. The portal is capable of merging data from multiple geographies or technologies into a common interface, allowing for comprehensive analysis, alerting, remediation, and reporting.

The Virtual-SOC provides real-time access for communications including ticket creation, event handling, incident response, data presentation, report generation, and trend analysis.

Reporting

The Customer will have access to comprehensive service information, through the Virtual-SOC, to review service tickets and Security Incidents at any time. One time per month, IBM will produce a summary report that includes:

a. number of SLAs invoked and met;

b. number and type of service requests;

c. list and summary of service tickets;

d. number of Security Incidents detected, priority and status; and

e. list and summary of Security Incidents.

2.3 Ongoing Management and Support – Package-Specific

The terms and conditions set forth in this section entitled "Ongoing Management and Support – Platform-Specific" apply to either the Protection or the Content package of MSS for UTM (as specified below). Except as further specified below, the terms and conditions set forth in this section apply to all three service levels (Standard, Select, and Premium).

2.3.1 Intrusion Prevention

The terms and conditions set forth in this section entitled "Intrusion Prevention" will apply only to Customers who have contracted for the MSS for UTM Protection package.

Intrusion Prevention technology allows the Agent to identify attacks. If the Agent is installed inline, it can help block network attacks.

Policy Management

IBM will configure and maintain an Intrusion Prevention policy, based on the Agent and service level purchased, enabling new security checks following the release of Security Content updates.

By default, policies are configured to detect and block critical attack activity, exploits associated with mass-propagating worms, and denial of service ("DoS") signatures. If such configuration causes undesirable results (e.g., a high number of false positives, irrelevant data, or the inadvertent blocking of legitimate traffic), IBM may take proactive measures to adjust the Agent's configuration. Such changes are necessary as excessive amounts of IDS/IPS data can cloud actual attack activity or impact the overall performance of a device.

MSS for UTM Customers at the Premium service level may also take advantage of multiple policy support on certain UTM Appliances. If the deployed platform provides such capability, and barring any technical or environmental limitations, Customers may deploy the device in a configuration which allows for a maximum of one policy per port pair when the device is deployed in an inline configuration. Additional policies may result in additional recurring monthly service fees.

Monitoring and Escalations

All attacks identified by the Agent's policy will be reported through the Virtual-SOC, including comprehensive data. If the Agent is deployed inline with Intrusion Prevention functionality, many of these attacks will have been blocked, and require no further action. As malicious activity occurs 24 hours/day by 7 days/week and blocked traffic is a regular occurrence, no escalations will follow the successful inbound block of unwanted traffic.

IBM also supports automated analysis for certain platforms. For these supported Agents, IBM will generate alerts based on incoming security events. These security events will be raised to the attention of an IBM analyst for review. Actionable, validated attacks will be treated as Security Incidents and will then be escalated to the designated Customer contacts via e-mail and/or e-mail-based text messaging notification.

The Virtual-SOC allows Customers to view and report on these alerts, and provides a full-featured ticketing system for handling and escalating Security Incidents internally.

Full Monitoring (Optional)

Policies watch for critical events, as well as medium- and low-priority malicious activity, suspicious activity, and network misuse. The Customer may request policy changes to enable additional detection or prevention capabilities, modify response actions, and fine tune the type of information received by the Intrusion Prevention module.

If the deployed Agent is capable of handling multiple policy support, and barring any technical or environmental limitations, the Customer may deploy the Agent in a configuration which allows for a maximum of one policy per port pair when the Agent is deployed in an inline configuration. Additional policies beyond these stated maximums may result in additional recurring monthly service fees.

IBM will monitor all security events generated by the Agent, validate the events and, if necessary, create a Security Incident ticket 24 hours/day by 7 days/week.

Monitoring Options		
Feature	**Reporting Only**	**Full Monitoring**
24 x 7 security event monitoring	Automated monitoring via intelligent systems	Automated monitoring with real-time 24 x 7 human analyses
Security Incident escalations	Via e-mail following identification and validation	Via telephone and/or e-mail, based on event priority
IDS/IPS policy configuration	High priority malicious activity	High, medium, and low-priority activity (including suspicious activity and network misuse)

2.3.2 Firewall

The terms and conditions set forth in this section entitled “Firewall” will apply only to Customers who have contracted for the MSS for UTM Protection package.

The firewall module is designed to prevent unwanted and malicious traffic from entering or leaving the enforcement point. The service identifies and blocks access to certain applications and data attempting to enter the Customer’s network, using stateful inspection (also called “dynamic packet filtering”).

Security Policy

During the initial setup and deployment process, IBM will work with the Customer to create a policy that is customized to the organization’s specific needs. Firewall module policies will support the creation of standard rules (e.g., source, destination, service, and action), object and protocol groupings, and network/port address translation configurations.

A single firewall policy/configuration change is defined as any authorized request for the addition or modification of one rule with five or fewer network or IP objects in a single request. Any change request requiring the addition of six or more network or IP objects or the manipulation of two or more rules will be counted as two or more requests. If the request applies to changes outside of the rule-based firewall policy, each submitted request will be considered a single change, within reasonable limits.

Authentication Accounts

Specific firewall functionality often allows for the authentication of user accounts to enable access through application proxies or for usage of specific protocols. IBM will support the enablement of such functionality; however, user account management is the responsibility of the authorized Customer security contacts. To simplify such a process, Customers may wish to integrate a third party authentication server with the firewall. Such server will be managed by the Customer and will simplify the process of account management by expanding available options for user administration. IBM issues surrounding authentication of protocols and application proxies also extend to client and SSL VPN capabilities.

Notifications and Alerts

Certain firewall platforms allow e-mails and/or SNMP traps to be generated and sent from the device when certain firewall-related events occur. By following the standard change request procedure, the Customer may request that IBM configure the firewall platform to deliver e-mails to a designated address, or generate SNMP traps.

Such a configuration is subject to approval by IBM, which will not be unreasonably withheld. However, among other reasons, a request will be denied if the configuration will have an adverse impact on the ability of the platform to protect the network environment. As with other device configurations, changes to the platform notification and alerting settings will be considered a policy change request.

2.3.3 VPN Support

The terms and conditions set forth in this section entitled "VPN Support" will apply only to Customers who have contracted for the MSS for UTM Protection package.

The VPN feature allows supported server-based or client-based VPNs to be connected to the Agent and helps to enable secure transmission of data across untrusted networks, via site-to-site communication. The default configuration of this feature activates this capability on the managed Agent and includes the initial configuration of up to two remote sites. After the initial configuration, each setup of a site-to-site VPN is considered a policy change.

IBM will support static authentication methods for both site-to-site and client VPN configurations. Static authentication also includes the use of the Customer's existing radius authentication server implementation. Certificate-based authentication is not currently supported as a part of the VPN service configuration.

Site-to-Site VPNs

A site-to-site VPN is defined as a VPN created between the Agent and another supported encryption device. Site-to-site VPNs provide help to secure connectivity for entire networks by building a tunnel between the managed firewall platform and another compatible VPN endpoint. Site-to-site VPNs can be established between:

- two IBM-managed VPN-capable Agents, or
- an IBM-managed endpoint and a non-IBM-managed endpoint. A one-time fee will be charged for the initial configuration of a managed to unmanaged endpoint.

In the event problems with the VPN tunnel arise after setup, IBM will work with the Customer and vendor contacts to identify, diagnose, and resolve performance and IBM-related issues.

Client VPNs

Client VPNs help to provide secure connectivity into a protected network, from a single workstation with the appropriate client VPN software and access credentials. Client VPNs help to enable remote workers to access internal network resources without the risk of eavesdropping or data compromise. For MSS for UTM Customers, the allowed number of simultaneous client VPN connections is as follows:

- Standard level – up to 20
- Select level - up to 50
- Premium level – unlimited (within platform constraints)

IBM supports client VPN implementations through an enablement model. IBM will work with the Customer to configure and test the first five client VPN users. Following successful connectivity for these five users, it will be the Customer's responsibility to perform user administration for individuals requiring a client VPN connection. IBM will provide the Customer with a demonstration of the user management capabilities of the deployed firewall platform (if applicable), and help to provide the appropriate access levels and software required to complete the setup.

Client VPN solutions typically require the installation of a client VPN application onto the specific workstations participating in the secured tunnel. The deployed Agent is designed to determine the specific client VPN applications to be supported. Some client VPN applications may be available through their respective vendors at no additional cost, while others are licensed per seat. The Customer is solely responsible for the acquisition, installation, and associated costs therein of any required client VPN software.

SSL VPNs

SSL VPNs are a type of client VPN, and each SSL VPN counts towards the client VPN allotment.

SSL VPNs help to offer secure connectivity into company resources from any Web-enabled personal computer ("PC"), without the need for a dedicated client VPN application. This allows remote workers to access company resources from an Internet-connected PC. In contrast to traditional Internet Protocol Security ("IPsec") VPNs, SSL VPNs do not require installation of specialized client software on users' computers.

IBM supports SSL VPN implementations through an enablement model. IBM will work with the Customer to configure and test the first five SSL VPN users. Following successful connectivity for these five users, it will be the Customer's responsibility to perform user administration for individuals requiring an SSL VPN connection. IBM will provide the Customer with a demonstration of the user management capabilities of the deployed firewall platform (if applicable), and provide the appropriate access levels and software required to complete the setup.

2.3.4 Web Filtering

The terms and conditions set forth in this section entitled "Web Filtering" will apply only to Customers who have contracted for the MSS for UTM Content package.

Web filtering is designed to address potential objectionable Internet content. Using content analysis technology, the managed Agent can provide policy-based content control.

Enabling Web filtering may require additional licensing for the Agent which shall be the sole responsibility of the Customer.

Configuration

In order for Web filtering to be effective, the Agent must be placed in a location where user Web traffic passes through the device(s) prior to reaching the intended destination. This allows the Web filtering module to compare the requested URL against the content database to validate the requested destination is authorized.

During the initial setup and deployment process, IBM will work with the Customer to create a policy that is customized to the organization's specific needs. Following is a general overview of features that extend across all supported Web filtering solutions:

- Category lists – a selection of content categories to block;
- Destination white lists – specific sites that should be allowed even if they exist within a denied content category;
- Destination blacklists – specific sites that should be blocked even if they exist within an allowed content category; and
- Source white list – specific IP addresses that should be excluded from content filtering.

2.3.5 Antispam

The terms and conditions set forth in this section entitled "Antispam" will apply only to Customers who have contracted for the MSS for UTM Content package.

The integrated antispam capabilities of many Agents check inbound and outbound e-mail messages for known spam signatures, patterns, and behaviors. The Agent must be placed in a location where e-mail passes through the device prior to reaching the mail gateway. This helps prevent undesirable messages from impacting the performance and availability of the mail gateway. While the core function of antispam technology is to eliminate unsolicited advertisements, most antispam technology also filters phishing attempts (i.e., e-mails designed to fool users into releasing their private data). Typically, phishing e-mails claim to be from a legitimate service, but refer the user to a malicious Web site which collects the user's personal data.

The antispam policy can typically be configured to white list or blacklist specific e-mail addresses and domains, as desired. Such configurations are designed to allow for e-mail messages from these e-mail addresses and domains to always pass, or always be deleted by the antispam module, respectively. IBM will work directly with the Customer to collect data required for IBM to construct customized white and blacklists tailored to the specific needs of the Customer.

Enabling antispam functionality may require additional licensing from the Agent's vendor, which shall be the sole responsibility of the Customer.

2.3.6 Antivirus

The terms and conditions set forth in this section entitled “Antivirus” will apply only to Customers who have contracted for the MSS for UTM Content package.

Antivirus support is designed to minimize the risk of malicious code within the network data stream. Antivirus gateways can be configured to scan Web, e-mail, and file-transfer traffic, and are designed to block the transmission of files which contain any of a number of designated threats. Most antivirus scanners will also block common forms of spyware, as well as many types of network worms.

Enabling antivirus functionality may require additional licensing for the Agent, which shall be the sole responsibility of the Customer.

Configuration

In order for antivirus implementations to be effective, the Agent must be placed in a location where user and inbound traffic passes through the device(s) prior to reaching its intended destination. This allows the Agent to compare monitored traffic against known virus signatures and/or behavior.

During the initial setup and deployment process, IBM will work with the Customer to create a policy that is customized to the organization’s specific needs.

3. Customer Responsibilities

While IBM will work with the Customer to deploy and implement the Agent, and IBM will manage the Agent, the Customer will be required to work with IBM in good faith and assist IBM in certain situations as requested by IBM.

3.1 Deployment and Initiation

During deployment, the Customer will work with IBM to deploy a new Agent or begin management of an existing Agent, as applicable.

The Customer will participate in a scheduled kickoff call to introduce team members, set expectations and begin the assessment process.

The Customer will be required to complete a form to provide detailed information about the network configuration (including applications and services for the Hosts on the protected network) and must work with IBM in good faith to accurately assess the Customer’s network and environment. The Customer must provide contacts within the organization, and specify an escalation path through the organization in the event that IBM must contact the Customer.

The Customer must ensure that any existing Agent meets IBM specifications, and must work to meet recommendations concerning the Customer’s network and network access requirements, if changes are required to ensure workable protection strategies.

If IBM will be taking over management of an existing Agent, IBM may require the Agent software or Security Content to be upgraded to the most current versions in order to provide the service. Other required criteria may include the addition or removal of applications and user accounts. Such upgrades, additions, or removals will be the sole responsibility of the Customer.

While IBM will provide support and guidance, the Customer is responsible for the physical installation and cabling of all Agents, unless such service is provided as an IBM PSS consulting project. If the Customer chooses to deploy the client VPN functionality of the Proventia MX, the Customer is responsible for the actual installation and some testing of the client VPN software, with IBM support. The Customer is responsible for procuring any client VPN software directly from a vendor, although IBM may make recommendations and guide the Customer to an appropriate vendor contact.

3.2 Ongoing Management and Support

3.2.1 Policy Management

The Customer acknowledges that IBM is the sole party responsible for and possessing authority to change the Agent’s policy and/or configuration.

While IBM may assist, the Customer is ultimately responsible for its own network security strategy, including incident response procedures such as forensics and mitigation of intrusions..

3.2.2 Device Management

If the Customer wishes to enable the HA feature of MSS for UTM, the Customer agrees to purchase a second Agent and pay for the ongoing management of such Agent.

The Customer is responsible for maintaining current hardware and software maintenance contracts.

Physical Environment

The Customer must provide a secure, physically controlled environment for the Agent.

Customers at the Standard service level who choose not to deploy an OOB solution may be required to provide hands-on assistance with the Agent for the purposes of troubleshooting and/or diagnosing technical difficulties.

Customers at the Select and Premium service levels must deploy an OOB solution.

On an annual basis, the Customer agrees to work with IBM to review the current hardware configuration of the managed devices and identify required updates. These updates will be based on identified changes to the OS and application requirements.

Network Environment

The Customer is responsible for making agreed-to changes to the network environment based upon IBM recommendations.

The Customer is required to maintain an active and fully functional Internet connection at all times, and must ensure the Agent is Internet-accessible via a dedicated, static IP address. Internet access service and telecommunications transport circuits are solely the Customer's responsibility.

The Customer is responsible for ensuring the desired network traffic and applicable segments are configured to route network traffic through the Agent.

Management Platforms

Customers hosting their own SiteProtector infrastructure:

a. must set up an event stream to IBM, via the Internet;

b. must ensure their Event Collectors have unique, routable IP addresses to forward events to IBM;

c. must have an Event Collector dedicated to the devices IBM will be monitoring on behalf of the Customer. Such Event Collector may not receive events from devices for which the Customer has not contracted for management or monitoring;

d. must provide IBM with full administrative access to the SiteProtector application server, via the SiteProtector console, for the purpose of pushing updates and controlling policy;

e. may be required to upgrade their SiteProtector infrastructure in order to transfer data to the IBM Managed Security Services infrastructure; and

f. must not alter the Agent's policy or configuration outside of the established policy change request procedure.

3.2.3 VPN Support

For VPN connections to sites that are not being managed by IBM, the Customer must provide a completed "VPN Site Configuration" form. The VPN will be configured in accordance with the information provided. Troubleshooting of remote site connectivity is strictly limited to IBM managed sites.

3.2.4 Data Gathering

The Customer consents to IBM gathering security event log data to look at trends, and real or potential threats. IBM may gather this security event log data with similar data of other clients so long as such data is gathered in a manner that will not in any way reveal the data as being attributable to the Customer.

4. Service Level Agreements for MSS for UTM for Standard, Select, and Premium Service Levels

IBM SLAs establish response time objectives and countermeasures for Security Incidents resulting from MSS for UTM. The SLAs become effective when the deployment process has been completed, the device has been set to "live", and support and management of the device have been successfully transitioned to the SOC.

The SLA remedies are available provided the Customer meets its obligations as defined in this Service Description.

4.1 SLA Guarantees

The SLA guarantees described below comprise the measured metrics for delivery of MSS for UTM. Unless explicitly stated below, no additional guarantees or warranties of any kind shall apply to services delivered under MSS for UTM. The remedies for failure to meet the SLA guarantees are specified in the section entitled "SLA Remedies", below.

a. Security Incident identification guarantee (available for the full monitoring service option only) – IBM will identify all Priority 1, 2, and 3 level Security Incidents based on Agent event data received by the SOCs. IBM will determine if an event is a Security Incident, based on the Customer's business requirements, network configuration, and Agent configuration.

b. Security Incident response guarantee (applies to all service levels, with or without the full monitoring service option) - IBM will respond to all identified Security Incidents as follows:

   (1) Reporting only service option – IBM will respond to all identified Security Incidents within 30 minutes of identification. The Customer's designated Security Incident contact will be notified via e-mail for Priority 1, 2 and 3 Security Incidents.

   (2) Full monitoring service option - IBM will respond to all identified Security Incidents within 15 minutes of identification. The Customer's designated Security Incident contact will be notified by telephone for Priority 1 Security Incidents and via e-mail for Priority 2 and 3 Security Incidents. During a Priority 1 Security Incident escalation, IBM will continue attempting to contact the designated Customer contact until such contact is reached or all escalation contacts have been exhausted.

   Operational activities related to Security Incidents and responses are documented and time-stamped within the IBM trouble ticketing system, which shall be used as the sole authoritative information source for purposes of this SLA guarantee.

c. Policy change request acknowledgement guarantee – IBM will acknowledge receipt of the Customer's policy change request within two hours of receipt by IBM. This guarantee is only available for policy change requests submitted by a valid security contact in accordance with the provided procedures.

d. Policy change request implementation guarantee:

   (1) Standard level - the Customer policy change requests will be implemented within 24 hours of receipt by IBM unless the request has been placed in a "hold" status due to insufficient information required to implement the submitted policy change request.

   (2) Select and Premium levels - the Customer policy change requests will be implemented within eight hours of receipt by IBM unless the request has been placed in a "hold" status due to insufficient information required to implement the submitted policy change request.

   This guarantee is only available for policy change requests submitted by a valid security contact in accordance with established procedures. Further, this guarantee is based on actual time of implementation, and not on the time that the Customer was notified the request was completed.

e. Emergency change request implementation guarantee (available for the Premium service level only) – IBM will implement Customer emergency policy change requests within two hours of the Customer's declaration of emergency (by telephone) following change submission through the Virtual-SOC.

   This guarantee is only available for policy change requests submitted by a valid security contact in accordance with established procedures. Further, this guarantee is based on actual time of implementation, and not on the time that the Customer was notified the request was completed.

   IBM will promptly notify the Customer upon implementation of a change request by telephone, e-mail, fax, pager, or electronic response via the Virtual-SOC and will continue attempting to contact the designated Customer contact until a contact is reached or all escalation contacts have been exhausted.

f. Proactive system monitoring guarantee:

   (1) Standard level - the Customer will be notified within 30 minutes after IBM determines the Customer's managed UTM device is unreachable via standard in-band connectivity.

(2) Select and Premium levels - the Customer will be notified within 15 minutes after IBM determines the Customer's managed UTM device is unreachable via standard in-band connectivity.

IBM will contact the designated Customer contact by a method elected by IBM. During an outage escalation, IBM will continue attempting to contact the designated Customer contact until such contact is reached or all escalation contacts have been exhausted.

g. Proactive Security Content update guarantee:

(1) Standard level – IBM will begin application of new Security Content updates within 72 hours after the update is published as generally available by the vendor.

(2) Select and Premium levels - IBM will begin application of new Security Content updates within 48 hours after the update is published as generally available by the vendor.

Table 3 – SLA Summary

Service Level Agreement	Standard	Select	Premium
Security Incident identification guarantee (for full monitoring option only)	Applicable		
Security Incident response guarantee	Reporting only option - response within 30 minutes Full monitoring option – response within 15 minutes		
Policy change request acknowledgement guarantee	Acknowledgement within 2 hours of receipt		
Policy change request implementation guarantee	Implementation within 24 hours of receipt	Implementation within 8 hours of receipt	Implementation within 8 hours of receipt
Emergency change request implementation guarantee	Not available	Not available	Implementation within 2 hours of declaration of emergency
Proactive Agent monitoring guarantee	Notification within 30 minutes	Notification within 15 minutes	
Proactive Security Content update guarantee	Begin updates within 72 hours	Begin updates within 48 hours	

4.2 SLA Remedies

As the sole remedy for failure to meet any of the guarantees described in the section entitled "SLA Guarantees", IBM will credit the Customer's account if IBM fails to meet the SLA guarantees described in the section entitled "SLA Guarantees" during any given calendar month. For all SLAs, the Customer may obtain no more than one credit for each SLA per day, not to exceed a total for all SLAs of $25,000 (U.S.), or the equivalent in local currency, in a given calendar month, as stated in the section entitled "SLA Exclusions and Stipulations" below. Specific SLA remedies are listed below:

- Security Incident identification, Security Incident response, policy change request acknowledgement, policy change request implementation, emergency change request implementation, proactive system monitoring and proactive Security Content update remedies – If IBM fails to meet any of these guarantees, the Customer account will be credited the applicable charges for one day of the monthly monitoring fee for the affected device.

Table 4 - SLAs and Remedies Summary

Service Level Agreements	Remedies for MSS for UTM (all service levels)
Security Incident identification guarantee	

Security Incident response guarantee	Credit of 1 day of the monthly monitoring fee for the package and service level of MSS for UTM for which the Customer has contracted.
Policy change request acknowledgement guarantee	
Policy change request implementation guarantee	
Emergency change request implementation guarantee (Premium level only)	
Proactive system monitoring guarantee	
Proactive Security Content update guarantee	

4.3 Scheduled and Emergency Portal Maintenance

Scheduled maintenance shall mean any maintenance:

a. of which the Customer is notified at least five days in advance; or

NOTE TO COUNTRY C&N: Replace "8:00 a.m. – 4:00 p.m. ET" with your local equivalent.

b. that is performed during the standard monthly maintenance window on the second Saturday of every month from 8:00 a.m. – 4:00 p.m. ET. Notice of scheduled maintenance will be provided to the designated Customer contact.

No statement in the section entitled "Service Level Agreements" shall prevent IBM from conducting emergency maintenance on an "as needed" basis. During such emergency maintenance, the affected Customer's primary point of contact will receive notification within 30 minutes of initialization of the emergency maintenance and within 30 minutes of the completion of any emergency maintenance.

4.4 SLA Exclusions and Stipulations

4.4.1 Customer Contact Information

Multiple SLAs require IBM to provide notification to the designated Customer contact after certain events occur. In the case of such an event, the Customer is solely responsible for providing IBM with accurate and current contact information for the designated contact(s). The current contact information on record is available to authorized contacts through the Virtual-SOC. IBM will be relieved of its obligations under these SLAs if IBM contact information is out of date or inaccurate due to Customer action or omission.

4.4.2 Customer Network/Server Change Notifications

The Customer is responsible for providing IBM advance notice regarding any network or server changes to the firewall environment. If the event advance notice cannot be provided, the Customer is required to provide IBM with notification of changes within seven calendar days of said network or server changes. Notification is completed by the submission or update of a critical server ticket through the Virtual-SOC. If the Customer fails to notify IBM as stated above, all SLA remedies are considered null and void.

4.4.3 Maximum Penalties/Remedies Payable to Customer

The total SLA credits (called "remedies") provided by MSS for UTM, described in the sections entitled "SLA Guarantees" and "SLA Remedies" above, will not exceed the service fees for one calendar month.

4.4.4 Network Traffic Applicable to SLAs

Certain SLAs focus on the prevention, identification and escalation of Security Incidents. These SLAs assume that traffic has successfully reached the firewall and therefore the firewall has the ability to process the traffic against the installed policy and generate a logged event. Traffic that does not logically or electronically pass through a firewall, or that does not generate a logged event, is not covered under these SLAs.

4.4.5 SLA Compliance and Reporting

SLA compliance and the associated remedies are based on fully functional network environments, Internet and circuit connectivity, firewalls, and properly configured servers. If SLA compliance failure is caused by CPE hardware or software (including any and all Agents), all SLA remedies are considered null and void. IBM will provide SLA compliance reporting through the Virtual-SOC.

4.4.6 Testing of Monitoring and Response Capabilities

The Customer may test IBM monitoring and response capabilities by staging simulated or actual reconnaissance activity, system or network attacks, and/or system compromises. These activities may be initiated directly by the Customer or by a contracted third party with no advance notice to IBM. SLAs will not apply during the period of such staged activities, and remedies will not be payable if the associated guarantee(s) are not met.

5. Service Level Objectives

IBM service level objectives (called "SLOs") establish nonbinding objectives for the provision of certain features of MSS for UTM. The SLOs become effective when the deployment process has been completed, the device has been set to "live", and support and management of the device have been successfully transitioned to the SOC. IBM reserves the right to modify these SLOs with 30 days prior written notice.

a. Virtual-SOC – IBM will provide a 99.9% accessibility objective for the Virtual-SOC outside of the times detailed in the section entitled "Scheduled and Emergency Portal Maintenance".

b. Internet Emergency – In the event IBM declares an Internet emergency, it is IBM's objective to notify the Customer's specified points of contact via e-mail within 15 minutes of emergency declaration. This notification will include an incident tracking number, telephone bridge number, and the time that IBM will conduct a situation briefing.

   During declared Internet emergencies, IBM will provide a live telephone-conference situation briefing and summarized e-mail designed to provide information that the Customer can use to protect their organization. Situation briefings following the onset of an Internet emergency will supersede any requirement for IBM to provide Customer-specific escalations for events directly related to the declared Internet emergency. IBM will communicate all other priority level incidents, during an Internet emergency, via automated systems such as e-mail, pager and voice mail.

   Standard escalation practices will resume upon conclusion of the stated Internet emergency. Termination of an emergency state is marked by a decrease in the AlertCon level to AlertCon 2, or an e-mail notification delivered to an authorized Customer security contact.

6. Other Terms and Conditions

IBM reserves the right to modify the terms of this Service Description, including the SLAs, with 30 days prior written notice.